CLAIMS:

1. A method for restoring previously un-backed up data during a system restore comprising the steps of:

storing backup files in a locked partition of a storage device;

starting restoration of said system;

reading other partitions of said storage device to determine which files have been modified since most recent backup operation;

running a virus scan on files determined to be modified;

uncorrupting modified files containing a virus that can be uncorrupted;

copying uncorrupted modified files; and

replacing backup files in said locked partition of said storage device that have been modified since most recent backup operation with said uncorrupted modified files.

2. The method as recited in claim 1 further comprising the step of:

restoring files of said system with said backup files stored in said locked partition of said storage device.

3. The method as recited in claim 1 further comprising the step of:

destroying modified files containing a virus that cannot be uncorrupted.

4. The method as recited in claim 1 further comprising the step of:

downloading an updated virus template into said locked partition of said storage device if a virus template needed to be updated.

5. The method as recited in claim 1, wherein said step of copying uncorrupted modified files comprises the steps of:

copying modified files with no detected viruses; and

copying modified files with a detected virus but cleaned by said virus scan.

6. The method as recited in claim 1 further comprising the steps of:

running said virus scan on files to be backed up prior to storing said backup files in said locked partition of said storage device; and

uncorrupting said files to be backed up containing a virus that can be uncorrupted prior to storing said backup files in said locked partition of said storage device;

wherein said backup files that are stored in said locked partition of said storage device are said files to be backed up with no detected virus and said files to be backed up with a detected virus but cleaned by said virus scan.

7. A computer program product embodied in a machine readable medium for restoring previously un-backed up data during a system restore comprising the programming steps of:

storing backup files in a locked partition of a storage device;

starting restoration of said system;

reading other partitions of said storage device to determine which files have been modified since most recent backup operation;

running a virus scan on files determined to be modified;

uncorrupting modified files containing a virus that can be uncorrupted;

copying uncorrupted modified files; and

replacing backup files in said locked partition of said storage device that have been modified since most recent backup operation with said uncorrupted modified files.

8. The computer program product as recited in claim 7 further comprising the programming step of:

restoring files of said system with said backup files stored in said locked partition of said storage device.

9. The computer program product as recited in claim 7 further comprising the programming step of:

destroying modified files containing a virus that cannot be uncorrupted.

10. The computer program product as recited in claim 7 further comprising the programming step of:

downloading an updated virus template into said locked partition of said storage device if a virus template needed to be updated.

11. The computer program product as recited in claim 7, wherein said programming step of copying uncorrupted modified files comprises the programming steps of:

copying modified files with no detected viruses; and

copying modified files with a detected virus but cleaned by said virus scan.

12. The computer program product as recited in claim 7 further comprising the programming steps of:

running said virus scan on files to be backed up prior to storing said backup files in said locked partition of said storage device; and

uncorrupting said files to be backed up containing a virus that can be uncorrupted prior to storing said backup files in said locked partition of said storage device;

wherein said backup files that are stored in said locked partition of said storage device are said files to be backed up with no detected virus and said files to be backed up with a detected virus but cleaned by said virus scan.

13. A system, comprising:

a processor;

a first operating system running on said processor;

a storage medium coupled to said processor, wherein said storage medium comprises a locked partition configured to store a second operating system and backup files, wherein said locked partition is accessed only by said second operating system; and

a memory unit coupled to said processor, wherein said memory unit is operable for storing a computer program for restoring previously un-backed up data during a system restore;

wherein said processor, responsive to said computer program, comprises:

circuitry operable for starting restoration of said system;

circuitry operable for reading other partitions of said storage device to determine which files have been modified since most recent backup operation;

circuitry operable for running a virus scan on files determined to be modified;

circuitry operable for uncorrupting modified files containing a virus that can be uncorrupted;

circuitry operable for copying uncorrupted modified files; and

circuitry operable for replacing backup files in said locked partition of said storage device that have been modified since most recent backup operation with said uncorrupted modified files.

14. The system as recited in claim 13, wherein said processor further comprises:

circuitry operable for restoring files of said system with said backup files stored in said locked partition of said storage device.

15. The system as recited in claim 13, wherein said processor further comprises:

circuitry operable for destroying modified files containing a virus that cannot be uncorrupted.

16. The system as recited in claim 13, wherein said processor further comprises:

circuitry operable for downloading an updated virus template into said locked partition of said storage device if a virus template needed to be updated.

17. The system as recited in claim 13, wherein said circuitry operable for copying uncorrupted modified files comprises:

circuitry operable for copying modified files with no detected viruses; and

circuitry operable for copying modified files with a detected virus but cleaned by said virus scan.

18. The system as recited in claim 13, wherein said processor further comprises:

circuitry operable for running said virus scan on files to be backed up prior to storing said backup files in said locked partition of said storage device; and

circuitry operable for uncorrupting said files to be backed up containing a virus that can be uncorrupted prior to storing said backup files in said locked partition of said storage device;

wherein said backup files that are stored in said locked partition of said storage device are said files to be backed up with no detected virus and said files to be backed up with a detected virus but cleaned by said virus scan.

19. A system, comprising:

a first computing system comprising:

a processor;

a first operating system running on said processor; and

a memory unit coupled to said processor, wherein said memory unit is operable for storing a computer program for restoring previously un-backed up data during a system restore; and

a storage medium coupled to said first computing system, wherein said storage medium comprises a locked partition configured to store a second operating system and backup files, wherein said locked partition is accessed only by said second operating system; and

wherein said processor, responsive to said computer program, comprises:

circuitry operable for starting restoration of said system;

circuitry operable for reading other partitions of said storage device to determine which files have been modified since most recent backup operation;

circuitry operable for running a virus scan on files determined to be modified;

circuitry operable for uncorrupting modified files containing a virus that can be uncorrupted;

circuitry operable for copying uncorrupted modified files; and

circuitry operable for replacing backup files in said locked partition of said storage device that have modified since most recent backup operation with said uncorrupted modified files.